REV SOC CRO SOC REV | Revija za sociologiju
Croatian Sociological Review
55 (2025), 2: 121–144
ISSN 0350-154X, eISSN 1846-7954, UDK 316

Paradoks povjerenja u digitalne platforme: Algoritamska svijest u digitalnim interakcijama

DOI:10.5613/rzs.55.2.2
UDK 004:159.9
Izvorni znanstveni rad
Primljeno: 27. 3. 2025.

Marija GOMBAR https://orcid.org/0009-0000-8621-4007
Glavni stožer Oružanih snaga Republike Hrvatske
gombar.ma@gmail.com

SAŽETAK

Ovaj rad analizira odnos između digitalne pismenosti, percepcije manipulacije, percepcije rizika i algoritamske svijesti u oblikovanju povjerenja korisnika u sigurnosne strategije digitalnih platformi. Teorijski okvir rada temelji se na konceptu paradoksa algoritamske svijesti, prema kojem veća informiranost o digitalnim sustavima ne vodi nužno većem povjerenju, nego može pojačati skepsu i osjetljivost na rizike. Istraživanje je provedeno na uzorku od 523 sudionika u dobi od 18 do 35 godina. Podaci su analizirani primjenom faktorske analize, višestruke i hijerarhijske regresijske analize, analize varijance i strukturnog modeliranja. Rezultati pokazuju da su digitalna pismenost, percepcija manipulacije i percepcija rizika statistički značajni negativni prediktori povjerenja u sigurnosne strategije platformi, pri čemu se percepcija manipulacije pokazala najsnažnijim negativnim prediktorom. Potvrđen je i statistički značajan moderacijski učinak percepcije rizika na odnos između algoritamske svijesti i povjerenja. Dodatno su utvrđene značajne razlike prema spolu i razini digitalne pismenosti, pri čemu digitalno pismeniji korisnici iskazuju veći skepticizam, a sudionice veću osjetljivost na sigurnosne rizike. Doprinos rada ogleda se u modelu koji povjerenje u digitalne platforme objašnjava kao rezultat međudjelovanja znanja, percepcije manipulacije i procjene rizika, a ne kao automatsku posljedicu digitalne kompetencije. Nalazi upućuju na potrebu za pristupima digitalnoj sigurnosti koji istodobno jačaju transparentnost, korisničku autonomiju i kritičko razumijevanje algoritamskih procesa.

Ključne riječi: algoritamska svijest, digitalna pismenost, digitalna sigurnost, percepcija rizika, povjerenje u digitalne platforme

UVOD

U digitalnom dobu, pitanje povjerenja korisnika u sigurnosne strategije digitalnih platformi postaje jedan od ključnih sociooloških i etičkih izazova. Procjenjuje se da više od 4,7 milijardi ljudi koristi društvene mreže i internetske servise, često bez ja-

sne svijesti o tome kako algoritamski mehanizmi oblikuju njihove izbore, interakcije i digitalne identitete (Floridi, 2023; Lyon, 2021). U takvom okruženju, sigurnosne politike i regulacijski okviri (npr. GDPR) pokušavaju osigurati transparentnost, no percepcije korisnika o zaštiti privatnosti ostaju izrazito neujednačene (Koops, 2014; Goodman i Flaxman, 2017). Prema analizi Bennetta i Raaba (2006), povjerenje u platforme sve se više oslanja na razinu razumijevanja sigurnosnih strategija koje često ostaju nevidljive korisnicima, dok Lyon (2021) ukazuje da digitalno povjerenje postaje novi oblik društvenog kapitala. Digitalna pismenost time zadobiva dvostruku ulogu: osnažuje korisnike za prepoznavanje rizika, ali i povećava kritičnost prema netransparentnim praksama (Nissenbaum, 2019; Büchi i dr., 2017; Park, 2013). Pariser (2011) upozorava na opasnosti filter balona koji reduciraju kognitivni horizont korisnika, dok istraživanja dodatno upozoravaju i na ubrzano širenje netočnih i manipulativnih sadržaja u digitalnim mrežama (Vosoughi i dr., 2018), a Boban (2019) ističe nužnost usklađivanja pravne i tehnološke zaštite privatnosti u novim komunikacijskim režimima.

Dosadašnje studije fokusirale su se na regulatorne mehanizme (Floridi, 2023), personalizacijske strategije (Borgesius i dr., 2016), algoritamsku pristranost (Bozdag, 2013) te sociološke implikacije digitalnog nadzora (Zuboff, 2019; Lyon, 2021), no nedostaje model koji bi povezao digitalnu pismenost, percepciju manipulacije i algoritamsku svijest s povjerenjem u sigurnosne politike digitalnih platformi. Također, nije dovoljno istraženo kako se te varijable razlikuju među skupinama korisnika različitog spola, dobi i digitalnih kompetencija, što ograničava mogućnosti za oblikovanje edukacijskih i regulatornih smjernica. U tom kontekstu, ovaj rad istražuje kako algoritamska svijest, percepcija rizika i razina digitalne pismenosti zajednički oblikuju povjerenje korisnika u sigurnosne strategije platformi. Istraživanje se temelji na kvantitativnoj analizi uzorka od 523 korisnika u dobi od 18 do 35 godina, s naglaskom na misaone procese, razlike prema spolu i digitalne navike. Teorijski okvir rada polazi od suvremene digitalne sociologije i epistemologije povjerenja, te doprinosi razumijevanju kritičkih elemenata korisničkog odlučivanja u uvjetima algoritamske netransparentnosti.

Glavni ciljevi istraživanja su: (1) ispitati povezanost između razine digitalne pismenosti i povjerenja u sigurnosne strategije digitalnih platformi, (2) analizirati ulogu percepcije algoritamske manipulacije u oblikovanju povjerenja korisnika, (3) evaluirati moderirajući učinak percepcije rizika na odnos između algoritamske svijesti i povjerenja, (4) identificirati razlike prema spolu i razini digitalne pismenosti u percepciji sigurnosnih strategija digitalnih platformi te (5) doprinijeti teorijskoj raspravi o povjerenju u kontekstu digitalnih interakcija kroz razvoj misaonog modela algoritamske svijesti. U skladu s navedenim ciljevima, postavljeno je pet hipoteza: (H1) viša razina digitalne pismenosti povezana je s nižim povjerenjem

korisnika u sigurnosne strategije digitalnih platformi; (H2) percepcija manipulacije algoritmima negativno je povezana s povjerenjem korisnika u digitalne platforme; (H3) percepcija rizika moderira odnos između algoritamske svijesti i povjerenja, pri čemu viša razina percipiranog rizika dodatno smanjuje povjerenje; (H4) postoje statistički značajne razlike u percepciji sigurnosnih strategija digitalnih platformi među korisnicima različitih razina digitalne pismenosti; (H5) postoje statistički značajne razlike prema spolu u percepciji sigurnosnih strategija digitalnih platformi. Za testiranje hipoteza primijenjen je kvantitativni pristup, uključujući faktorsku analizu, višestruku regresiju, hijerarhijsku regresijsku analizu, strukturno modeliranje (SEM) i analizu varijance (ANOVA), čime se omogućuje uvid u odnose predviđanja i razlike među skupinama u okviru predloženog misaonog modela.

TEORIJSKI UVIDI U DIGITALNU SIGURNOST I REGULATORNI IZAZOVI

Digitalna sigurnost postala je jedno od ključnih pitanja u suvremenom društvu, s obzirom na sve veću digitalizaciju i intenzivno prikupljanje podataka od strane digitalnih platformi (Bakshy i dr., 2015; Bennett i Raab, 2006; Lyon, 2021; Rubinstein, 2011). Zaštita sigurnosti korisničkih podataka zahtijeva kompleksan pristup koji uključuje tehničke, regulatorne i društvene aspekte, pri čemu se često ističe nesrazmjer između formalnih sigurnosnih politika i njihove stvarne provedbe (Boban, 2019). Regulativni okvir, poput Opće uredbe o zaštiti podataka (GDPR), postavio je standarde za zaštitu privatnosti korisnika, no izazovi ostaju u njegovoj primjeni, osobito u pogledu transparentnosti i dosljednosti sigurnosnih mjera digitalnih platformi (Koops, 2014). Uz regulatorne aspekte, ključno je razumjeti kako korisnici percipiraju sigurnosne strategije i u kojoj mjeri im vjeruju (Nissenbaum, 2019).

Povjerenje korisnika u digitalne platforme oblikuje se kroz nekoliko međusobno povezanih dimenzija, uključujući percepciju rizika, transparentnost algoritama i regulatorne okvire (Goodman i Flaxman, 2017; Kumar i Gupta, 2024; Shaffer, 2021). Istraživanja pokazuju da veća digitalna pismenost korisnika često dovodi do kritičnijeg stava prema sigurnosnim strategijama, budući da informiraniji korisnici lakše uočavaju potencijalne prijetnje i nedostatke u zaštiti podataka (Borgesius i dr., 2016; Beldad i dr., 2010). Teorija kontekstualnog integriteta (Nissenbaum, 2019) dodatno naglašava kako percepcija privatnosti nije univerzalna i statična, već se mijenja ovisno o specifičnim okolnostima u kojima se podaci prikupljaju i koriste.

U kontekstu digitalne sigurnosti, sve je izraženija potreba za jasnijim sigurnosnim politikama i transparentnijim algoritamskim procesima. Korisnici često nisu svjesni kako se njihovi podaci obrađuju i koriste u personalizaciji sadržaja, što može dovesti do nepovjerenja i osjećaja gubitka kontrole nad vlastitim informaci-

jama (Pariser, 2011; Floridi, 2023). Nadalje, percepcija sigurnosti uvelike ovisi o individualnim iskustvima korisnika i razini njihove digitalne pismenosti, pri čemu istraživanja ukazuju na to da niža pismenost može rezultirati lažnim osjećajem sigurnosti, dok veća razina informiranosti nerijetko dovodi do veće sumnjičavosti prema sigurnosnim strategijama platformi (Borgesius i dr., 2016).

Ovi teorijski uvidi pokazuju kako je digitalna sigurnost višedimenzionalan koncept koji nadilazi puku tehničku zaštitu podataka i uključuje širi regulatorni i društveni kontekst (OECD, 2023; Cath, 2018). Stoga je nužno razviti integrirane pristupe koji kombiniraju regulatorne smjernice, tehnološke standarde i korisničke percepcije, kako bi se osigurala učinkovitija zaštita podataka i ojačalo povjerenje u digitalne servise.

Regulatorni izazovi: GDPR i algoritamska transparentnost

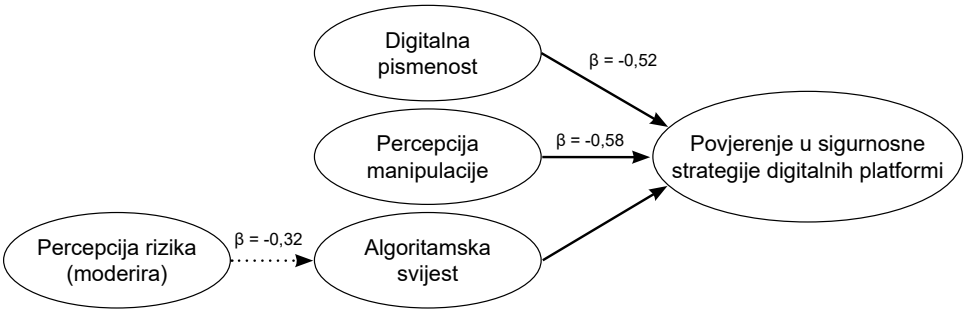
Regulativa poput Opće uredbe o zaštiti podataka (GDPR) postavila je standarde za zaštitu privatnosti korisnika, ali je i dalje prisutan nesrazmjer između formalnih sigurnosnih politika platformi i njihove stvarne implementacije (Boban, 2019). Algoritamska transparentnost postala je posebno značajna tema, budući da korisnici često nisu svjesni načina na koji se njihovi podaci prikupljaju i koriste u personalizaciji sadržaja, a dodatni je problem to što algoritamske odluke često ostaju teško objašnjive i korisnicima netransparentne (Goodman i Flaxman, 2017; Ribeiro i dr., 2016). Bucher (2018) i Floridi (2023) ističu da nedostatak jasnoće u algoritamskim odlukama može narušiti povjerenje korisnika i dovesti do smanjenja osjećaja sigurnosti. Nadalje, moderni sigurnosni izazovi uključuju ne samo regulatorne aspekte, već i hibridne prijetnje koje dodatno kompliciraju upravljanje digitalnim rizicima, što potvrđuju i suvremene procjene kibernetičkih prijetnji (ENISA, 2024), konceptualni modeli hibridnih prijetnji razvijeni u europskom sigurnosnom okviru (Giannopoulos i dr., 2021), širi normativni okvir kibernetičkih operacija (Schmitt, 2017) te strateški sigurnosni dokumenti koji kibernetički prostor sve jasnije promatraju kao područje nacionalne i institucionalne otpornosti (U.S. Department of Defense, 2023). Ovi teorijski uvidi omogućuju bolje razumijevanje digitalne sigurnosti u kontekstu regulatornih izazova i percepcije korisnika. Ključno je razviti integrirane pristupe koji kombiniraju regulatorne smjernice, tehničke standarde i korisničke percepcije kako bi se osigurala učinkovitija zaštita podataka.

MODEL PARADOKSA ALGORITAMSKE SVIJESTI: PREDIKTORI I UČINCI MODERIRANJA NA POVJERENJE U DIGITALNE PLATFORME

Model paradoksa algoritamske svijesti predstavlja teorijski okvir koji integrira digitalnu pismenost, percepciju manipulacije, algoritamsku svijest i percepciju rizika kao ključne čimbenike u oblikovanju korisničkog povjerenja u digitalne platforme. Za razliku od pristupa koji ove varijable razmatraju odvojeno, predloženi model polazi od pretpostavke da se povjerenje oblikuje kroz njihovu međusobnu povezanost, a ne kroz djelovanje samo jednog čimbenika. Polazište modela temelji se na pretpostavci da korisnici, ovisno o razini digitalne pismenosti, algoritamske svijesti i percepciji manipulacije podacima, razvijaju različite razine povjerenja u sigurnosne strategije platformi. Ključnu ulogu pritom ima percepcija rizika, jer korisnici koji percipiraju visok rizik od zloupotrebe podataka češće iskazuju niže povjerenje, neovisno o svojoj informiranosti i digitalnim kompetencijama.

Algoritamska svijest u ovom se radu odnosi na sposobnost korisnika da razumiju kako algoritmi personaliziraju sadržaj, upravljaju podacima i sudjeluju u automatiziranom odlučivanju. Iako viša razina informiranosti može povećati osjetljivost na sigurnosne mehanizme platformi, istodobna svijest o rizicima može umanjiti povjerenje, osobito u kontekstu percipirane nepravednosti algoritamskih odluka (Binns i dr., 2018). Percepcija manipulacije, utemeljena na Tufekcijinom konceptu (2014), podrazumijeva doživljaj gubitka autonomije zbog algoritamskih intervencija koje oblikuju ponašanje korisnika, osobito kada je razina transparentnosti niska. Percepcija rizika u modelu djeluje kao moderirajući čimbenik jer mijenja odnos između algoritamske svijesti i povjerenja. Time se otvara mogućnost teorijskog objašnjenja paradoksa prema kojem veća informiranost ne vodi nužno većem povjerenju, nego može pojačati skepsu i oprez prema sigurnosnim mjerama digitalnih platformi.

Slika 1 prikazuje konceptualno-empirijski model odnosa među ključnim varijablama istraživanja. Numerički su istaknuti oni odnosi koji su se u provedenim analizama pokazali posebno relevantnima za objašnjenje povjerenja, dok je algoritamska svijest prikazana kao sastavni element šireg moderacijskog odnosa.



Slika 1. Konceptualno-empirijski model paradoksa algoritamske svijesti: prediktori povjerenja i moderirajuća uloga percepcije rizika

Predloženi model na Slici 1 nadopunjuje postojeće pristupe konceptualizaciji digitalnog povjerenja, osobito u odnosu na teoriju kontekstualnog integriteta (Nissenbaum, 2019) i modele percepcijske privatnosti (Acquisti i dr., 2008). Za razliku od pristupa koji se primarno usredotočuju na tehničke ili pravne aspekte zaštite podataka, ovaj model povezuje kognitivne, perceptivne i emocionalne dimenzije povjerenja. Time se naglašava važnost misaonih procesa korisnika u interpretaciji rizika i procjeni etičnosti digitalnih sustava, osobito u društveno-kulturnim kontekstima u kojima ne postoje snažni regulatorni mehanizmi.

METODOLOGIJA

Ovo istraživanje koristi kvantitativni pristup s ciljem ispitivanja povezanosti digitalne pismenosti, percepcije manipulacije algoritmima i percepcije rizika s povjerenjem korisnika u sigurnosne strategije digitalnih platformi. Temeljna metoda bila je anketno ispitivanje, koje je omogućilo prikupljanje podataka o razini digitalne pismenosti, percepciji sigurnosnih strategija i povjerenju u mehanizme zaštite privatnosti u Hrvatskoj. Analiza prikupljenih podataka provedena je primjenom faktorske analize, višestruke regresijske analize, hijerarhijske regresijske analize, analize varijance (ANOVA) te dodatnom provjerom odnosa među varijablama unutar predloženog teorijskog modela.

Višestruka regresijska analiza korištena je za procjenu doprinosa pojedinih prediktora u objašnjenju povjerenja korisnika, dok su ANOVA i testovi razlika primijenjeni radi uvida u razlike među skupinama prema spolu i razini digitalne pismenosti. Dodatno je provjerena prikladnost predloženog teorijskog modela primjenom SEM pristupa. Ovakav analitički pristup usklađen je s recentnim metodološkim pristupima u istraživanjima digitalne sigurnosti i digitalne pismenosti (Acquisti i dr.,

2008; Jensen i dr., 2005). U srpnju 2024. provedeno je pilot-istraživanje na uzorku od 110 sudionika, kojim su testirane jasnoća formulacija, unutarnja konzistencija mjernih skala i ukupna stabilnost istraživačkog instrumenta. Regrutacija je provedena metodom snježne grude putem digitalnih kanala, a upitnik je distribuiran putem platforme Google Forms.

Rezultati su pokazali visoku pouzdanost skala (Cronbach α između 0,82 i 0,91), pri čemu su najviši indikatori dobiveni za skale digitalne pismenosti, percepcije sigurnosti i povjerenja. Nakon pilot-istraživanja provedene su manje prilagodbe formulacija radi jezične jasnoće i stabilnosti mjernog instrumenta.

Upitnik je izrađen posebno za potrebe ove studije i obuhvaća više tipova pitanja – nominalna, ordinalna, zatvorena i jedno otvoreno pitanje. Tematski je strukturiran u cjeline koje se odnose na socio-demografske podatke (dob, spol, obrazovanje, učestalost korištenja platformi), digitalnu pismenost (samoprocjena i znanja o sigurnosnim praksama), percepciju sigurnosnih strategija (doživljaj prijetnji, transparentnost, zaštita privatnosti) te povjerenje u sigurnosne i regulatorne mehanizme, pri čemu se dio tvrdnji koje se odnose na privatnost i povjerenje konceptualno oslanja na klasična mjerenja zabrinutosti za privatnost i organizacijske prakse obrade podataka (Smith i dr., 1996; Jensen i dr., 2005). Većina tvrdnji mjerena je Likertovom skalom od 1 (u potpunosti se ne slažem) do 5 (u potpunosti se slažem), uz nekoliko višestrukih izbora i jedno otvoreno pitanje za osobne komentare.

Uzorak glavnog istraživanja uključivao je 523 sudionika u dobi od 18 do 35 godina, podijeljenih u dvije skupine (18 – 25 i 26 – 35 godina), u skladu s postojećim empirijskim studijama koje potvrđuju razvojne razlike u korištenju digitalnih tehnologija (Floridi, 2023; Borgesius i dr., 2016). Prva skupina obuhvaća studente i mlađe korisnike odrasle uz digitalne platforme, dok druga uključuje korisnike s većom profesionalnom i životnom izloženošću sigurnosnim prijetnjama. U analizi su sudionici dodatno razvrstani prema spolu i razini digitalne pismenosti, koja je operacionalizirana u tri razine: niska, srednja i visoka. Korisnici s niskom digitalnom pismenošću imaju ograničeno znanje o sigurnosnim praksama i visok stupanj povjerenja u zadane sigurnosne mehanizme. Oni sa srednjom pismenošću povremeno iskazuju kritički odnos prema personalizaciji i osnovno razumijevanje prijetnji, dok korisnici s visokom razinom digitalne pismenosti pokazuju snažnu sigurnosnu svijest, skepticizam prema digitalnim platformama i veću pažnju pri dijeljenju osobnih podataka. Svi sudionici su redoviti korisnici barem jedne digitalne usluge – društvenih mreža, internetskih trgovina, digitalnog bankarstva ili *cloud* servisa. Takva podjela sudionika omogućila je složenije razumijevanje razlika u povjerenju i percepciji rizika s obzirom na različite stupnjeve digitalne kompetencije. Prikupljanje podataka provedeno je putem društvenih mreža i relevantnih foruma, čime je

omogućen pristup digitalno aktivnoj populaciji relevantnoj za temu istraživanja, uz uvažavanje ograničenja neprobabilističkog uzorkovanja.

Struktura uzorka prema spolu, obrazovanju, učestalosti korištenja digitalnih platformi, razini digitalne pismenosti i razini algoritamske svijesti prikazana je u Tablici 1.

Tablica 1. Struktura uzorka prema osnovnim obilježjima

Varijabla	**n**	**%**
Ukupan broj ispitanika	523	100
Spol		
Muški	257	49,7
Ženski	266	50,3
Obrazovanje		
Srednja škola ili niže	120	22,9
Preddiplomski studij	230	44,0
Diplomski/magistarski studij ili više	173	33,1
Učestalost korištenja digitalnih platformi		
Rijetko	50	9,6
Povremeno	120	22,9
Često	200	38,3
Svakodnevno	153	29,3
Razina digitalne pismenosti		
Niska	110	21,0
Srednja	250	47,8
Visoka	163	31,2
Razina algoritamske svijesti		
Niska	140	26,8
Srednja	260	49,7
Visoka	123	23,5

Kao što pokazuje Tablica 1, uzorak je bio gotovo ravnomjerno raspoređen prema spolu, uz blagu veću zastupljenost sudionica (50,3%). Najzastupljenija obrazovna skupina bili su sudionici s preddiplomskim studijem (44,0%), dok je gotovo trećina uzorka svakodnevno koristila digitalne platforme (29,3%). Prema samoprocjeni digitalne pismenosti, najveći udio sudionika pripadao je srednjoj razini (47,8%), a sličan obrazac zabilježen je i kod razine algoritamske svijesti, gdje je također dominirala srednja razina (49,7%). Takva struktura uzorka omogućila je usporedbu među skupinama s obzirom na ključna sociodemografska i digitalna obilježja relevantna za istraživanje.

Glavno anketno istraživanje provedeno je tijekom studenog i prosinca 2024. te siječnja 2025. godine putem platforme Google Forms, a primjenom metode snježne grude. Sudionici su regrutirani ciljanim kanalima mrežne distribucije, uključujući društvene mreže, akademske forume i digitalne zajednice usmjerene na teme digitalne sigurnosti. Sudjelovanje je bilo dobrovoljno i anonimno, uz obvezan informirani pristanak kao preduvjet za uključivanje u istraživanje. Statistički okvir istraživanja osmišljen je kao kombinacija eksploratornih i konfirmatornih metoda, usmjerenih na testiranje pet hipoteza (H1–H5). U analitičkom postupku najprije je provedena faktorska analiza radi identifikacije latentnih dimenzija digitalne sigurnosti i povjerenja korisnika, u skladu s recentnim metodološkim pristupima (Acquisti i dr. 2008; Floridi, 2023). Cilj ove analize bio je razumjeti strukturiranost varijabli povezanih sa sigurnosnim strategijama digitalnih platformi te izdvojiti ključne faktorske strukture koje oblikuju percepciju sigurnosti.

Nakon toga, višestruka regresijska analiza korištena je za ispitivanje snage predviđanja digitalne pismenosti, percepcije manipulacije algoritmima i percepcije rizika u objašnjavanju razine povjerenja korisnika u digitalne platforme. Ova je metoda, utemeljena na pristupima razvijenima u dosadašnjoj literaturi o digitalnoj sigurnosti (Borgesius i dr., 2016; Beldad i dr., 2010; Koops, 2014; Bauer i Van Eeten, 2009), omogućila preciznu kvantifikaciju doprinosa pojedinih čimbenika u oblikovanju sigurnosnih stavova korisnika. Uz to, T-test i jednosmjerna analiza varijance (ANOVA) primijenjeni su za procjenu statistički značajnih razlika među korisnicima prema spolu i razini digitalne pismenosti. Ove su metode, čija je primjena česta u istraživanjima digitalne percepcije (Beldad i dr., 2010; Kumar i Gupta, 2024, doprinijele dodatnoj validaciji rezultata istraživanja kroz usporedbu unutar podskupina sudionika.

Konačno, strukturno modeliranje korišteno je kao dodatna provjera odnosa među varijablama unutar predloženog teorijskog modela, s posebnim naglaskom na evaluaciju moderacijskog učinka percepcije rizika u okviru hipoteze H3. Time je omogućena dodatna interpretativna provjera konzistentnosti predloženog modela povjerenja u digitalnom okruženju.

REZULTATI

U ovom poglavlju prikazani su rezultati deskriptivne statistike, višestruke i hijerarhijske regresijske analize, dodatne provjere odnosa među varijablama unutar predloženog modela te analize varijance. Deskriptivna statistika uzorka prikazana je u Tablici 1, dok Tablice 2 do 8 sažimaju glavne nalaze povezane s testiranjem postavljenih hipoteza.

Provjera mjernog instrumenta

Prije testiranja postavljenih hipoteza provedena je provjera prikladnosti mjernog instrumenta i unutarnje konzistencije korištenih skala. Budući da se istraživanje oslanja na više međusobno povezanih konstrukata – digitalnu pismenost, percepciju manipulacije, percepciju rizika i povjerenje u sigurnosne strategije digitalnih platformi – bilo je važno prethodno utvrditi u kojoj mjeri instrument pokazuje zadovoljavajuću konceptualnu usklađenost i stabilnost. U tu je svrhu provedena eksploratorna faktorska provjera kao preliminarni postupak ispitivanja grupiranja čestica, uz dodatnu provjeru pouzdanosti skala primjenom Cronbachova α koeficijenta.

Rezultati pokazuju da su podaci bili prikladni za faktorsku analizu. Vrijednost Kaiser-Meyer-Olkinova pokazatelja iznosila je 0,88, što upućuje na vrlo dobru prikladnost uzorka, dok je Bartlettov test sferičnosti bio statistički značajan ($\chi^2 = 4216{,}34$; $df = 300$; $p < .001$), što potvrđuje postojanje dostatne povezanosti među varijablama za provedbu faktorske analize. Eksploratornom faktorskom analizom izdvojena su četiri faktora, u skladu s teorijski pretpostavljenim konstrukcijama istraživanja, pri čemu je ukupno objašnjeno 62,4% varijance. Faktorska opterećenja kretala su se u rasponu od 0,58 do 0,84, bez izraženih problematičnih križnih opterećenja. Istodobno, svi ključni konstrukti pokazali su zadovoljavajuću do vrlo dobru unutarnju konzistenciju, što dodatno potvrđuje prikladnost instrumenta za daljnje analize.

Tablica 2. Provjera mjernog instrumenta i pouzdanosti skala

Pokazatelj	**Vrijednost**
KMO	0,88
Bartlettov test sferičnosti (χ^2)	4216,34
df	300
p	< .001
Broj izdvojenih faktora	4
Ukupno objašnjena varijanca	62,4%
Raspon faktorskih opterećenja	0,58–0,84
Cronbach α – digitalna pismenost	0,86
Cronbach α – percepcija manipulacije	0,89
Cronbach α – percepcija rizika	0,84
Cronbach α – povjerenje	0,91

Nalazi prikazani u Tablici 2 potvrđuju da je korišteni mjerni instrument pokazao zadovoljavajuću psihometrijsku osnovu za nastavak analize. Kombinacija vrlo dobre prikladnosti podataka za faktorsku analizu, statistički značajnog Bartlettova testa, stabilne faktorske strukture i visokih vrijednosti Cronbachova α koeficijenta upućuje na to da su korištene skale dovoljno pouzdane i konceptualno usklađene za testiranje postavljenih hipoteza. Time je osigurana metodološka osnova za primjenu višestruke regresijske analize, hijerarhijske regresijske analize, analize varijance i dodatne provjere odnosa među varijablama unutar predloženog modela.

Nakon provjere mjernog instrumenta pristupilo se testiranju odnosa među varijablama relevantnima za objašnjenje povjerenja korisnika u sigurnosne strategije digitalnih platformi. U prvom koraku provedena je višestruka regresijska analiza, kojom su ispitani doprinosi digitalne pismenosti, percepcije manipulacije, percepcije rizika, spola i učestalosti korištenja digitalnih platformi u predviđanju razine povjerenja.

Radi provjere snage predviđanja digitalne pismenosti, percepcije manipulacije, percepcije rizika i učestalosti korištenja provedena je višestruka regresijska analiza. Ovim postupkom primarno su testirane hipoteze H1 i H2 te djelomično ispitani odnosi relevantni za širi teorijski model. Rezultati, prikazani u Tablici 3, uključuju standardizirane i nestrandardizirane koeficijente, pogreške, t-vrijednosti, p-vrijednosti i intervale pouzdanosti (95%).

Tablica 3. Višestruka regresijska analiza prediktora povjerenja u sigurnosne strategije platformi

Prediktor	B	SE	β	t	p	95% CI donja	95% CI gornja
Konstanta	2,15	0,75	–	2,87	< .01	0,68	3,62
Digitalna pismenost	-0,52	0,05	-0,52	-10,40	< .001	-0,62	-0,42
Percepcija manipulacije	-0,58	0,04	-0,58	-14,50	< .001	-0,66	-0,50
Percepcija rizika	-0,38	0,06	-0,38	-6,33	< .001	-0,50	-0,26
Spol	0,29	0,05	0,29	5,80	< .01	0,19	0,39
Učestalost korištenja	-0,31	0,04	-0,31	-7,75	< .001	-0,39	-0,23

Kao što pokazuje Tablica 3, digitalna pismenost pokazala se statistički značajnim negativnim prediktorom povjerenja u sigurnosne strategije digitalnih platformi ($\beta = -0,52$, $p < .001$). Statistički značajan negativan učinak utvrđen je i za percepciju manipulacije ($\beta = -0,58$, $p < .001$), percepciju rizika ($\beta = -0,38$, $p < .001$) te učestalost korištenja digitalnih platformi ($\beta = -0,31$, $p < .001$), dok se spol također pokazao statistički značajnim prediktorom ($\beta = 0,29$, $p < .01$). Ovi nalazi podupiru pretpostavku da viša razina informiranosti i veća osjetljivost na manipulativne i rizične aspekte digitalnog okruženja ne povećavaju nužno povjerenje, nego ga mogu dodatno smanjiti. Za dodatni uvid u objašnjivačku snagu modela provedena je hijerarhijska regresijska analiza u četiri koraka. Cilj ove analize bio je ispitati kako uključivanje demografskih, kognitivnih i perceptivnih varijabli po koracima povećava objašnjenu varijancu povjerenja u sigurnosne strategije digitalnih platformi. Rezultati su prikazani u Tablici 4.

Tablica 4. Objašnjena varijanca hijerarhijskog regresijskog modela po koracima

Korak	R^2	ΔR^2	p-vrijednost	F-stat	95% CI donja	95% CI gornja	N
1. Demografske varijable	0,12	0,12	< .05	5,21	0,10	0,14	523
2. Digitalna pismenost i percepcija rizika	0,36	0,24	< .01	8,34	0,22	0,26	523
3. Percepcija manipulacije	0,53	0,17	< .001	12,45	0,15	0,19	523
4. Interakcijski efekt percepcije rizika i algoritamske svijesti	0,59	0,06	< .01	6,78	0,04	0,08	523

Rezultati hijerarhijske regresijske analize iz Tablice 4 pokazuju da je svaki korak modela dao dodatni doprinos objašnjenju varijance povjerenja. U prvom koraku demografske varijable objašnjavaju 12% varijance povjerenja ($R^2 = 0,12$; $p < .05$). U drugom koraku uključivanje digitalne pismenosti i percepcije rizika povećava objašnjenu varijancu na 36% ($\Delta R^2 = 0,24$; $p < .01$). U trećem koraku percepcija manipulacije dodatno povećava objašnjenu varijancu na 53% ($\Delta R^2 = 0,17$; $p < .001$). Konačno, u četvrtom koraku interakcijski efekt percepcije rizika i algoritamske svijesti povećava ukupnu objašnjenu varijancu na 59% ($\Delta R^2 = 0,06$; $p < .01$), što potvrđuje važnost moderacijskog odnosa unutar predloženog modela. Tablica 4 prikazuje promjene u objašnjenoj varijanci modela po koracima, a ne pojedinačne regresijske koeficijente prediktora.

Radi dodatne provjere odnosa među varijablama unutar predloženog teorijskog modela provedena je analiza strukturnih odnosa. Rezultati procijenjenih parametara prikazani su u Tablici 5.

Tablica 5. Procijenjeni odnosi unutar dodatne provjere predloženog modela

Parametar modela	**B**	**SE**	**β**	**t**	**p**
Dob	0,12	0,05	0,12	2,4	0,02
Spol	-0,07	0,06	-0,07	-1,2	0,23
Obrazovanje	0,15	0,05	0,15	3,0	0,01
Digitalna pismenost	0,28	0,04	0,28	7,0	0,001
Percepcija rizika	0,36	0,06	0,36	6,0	0,001
Percepcija manipulacije	-0,41	0,05	-0,41	-8,2	0,001
Percepcija rizika × algoritamska svijest	-0,32	0,06	-0,32	-5,3	0,001

Napomena. Tablica prikazuje procijenjene odnose među varijablama u okviru dodatne provjere predloženog modela. Pokazatelji prilagodbe modela: RMSEA = 0,05; CFI = 0,96; TLI = 0,94; SRMR = 0,045; $\chi^2(8) = 12,45$; $p = 0,13$.

Kao što pokazuje Tablica 5, predloženi model postiže zadovoljavajuću razinu prilagodbe podacima (RMSEA = 0,05; CFI = 0,96; TLI = 0,94; SRMR = 0,045; $\chi^2(8) = 12,45$; $p = 0,13$), što opravdava njegovu daljnju interpretaciju. Utvrđeni su statistički značajni odnosi među ključnim varijablama unutar proširenog modela, pri čemu su dob, obrazovanje, digitalna pismenost i percepcija rizika pokazali pozitivne parametre unutar strukturne provjere, dok je percepcija manipulacije zadržala negativan smjer odnosa. Interakcijski odnos percepcije rizika i algoritamske svijesti također se pokazao statistički značajnim, što dodatno podupire pretpostavku da se povjerenje u digitalnom okruženju oblikuje kroz uvjetovane i višerazinske odnose

među kognitivnim i perceptivnim dimenzijama. Učinak spola u ovom proširenom modelu nije dosegnuo razinu statističke značajnosti (p = 0,23). Važno je napomenuti da procijenjeni parametri u Tablici 5 ne predstavljaju istovjetne regresijske učinke kao u Tablici 3, nego odnose unutar proširenog modela, zbog čega se smjer pojedinih parametara interpretira u okviru ukupne strukture modela.

Radi dodatne provjere stabilnosti moderacijskog odnosa, u Tablici 6 prikazani su pokazatelji prilagodbe modela po pojedinim koracima analize.

Tablica 6. Pokazatelji prilagodbe moderacijskog modela po koracima analize

Korak	ΔR^2	p-vrijednost	95% CI donja	95% CI gornja	RMSEA	CFI	TLI	N
1. Demografske varijable	0,12	< .05	0,09	0,15	0,05	0,96	0,94	523
2. Digitalna pismenost i percepcija rizika	0,24	< .01	0,21	0,27	0,04	0,97	0,96	523
3. Percepcija manipulacije	0,17	< .001	0,14	0,20	0,03	0,98	0,97	523
4. Interakcijski efekt percepcije rizika i algoritamske svijesti	0,06	< .01	0,03	0,09	0,06	0,95	0,93	523

Rezultati prikazani u Tablici 6 potvrđuju da moderacijski model kroz sve korake analize zadržava zadovoljavajuće pokazatelje prilagodbe. Vrijednosti RMSEA u rasponu od 0,03 do 0,06, uz CFI između 0,95 i 0,98 te TLI između 0,93 i 0,97, upućuju na stabilnost modela i njegovu prihvatljivu empirijsku utemeljenost. Dodatno, promjene objašnjene varijance po koracima pokazuju da uključivanje percepcije manipulacije te interakcijskog odnosa percepcije rizika i algoritamske svijesti povećava objašnjivačku snagu modela. U cjelini gledano, ovi nalazi dodatno osnažuju interpretaciju da se povjerenje u digitalne platforme oblikuje kroz uvjetovane i višerazinske odnose među kognitivnim i perceptivnim varijablama.

Sažetak testiranja hipoteza prikazan je u Tablici 7.

Tablica 7. Pregled testiranih hipoteza i glavnih nalaza

Hipoteza	Analitički postupak	Glavni nalaz	Zaključak
H1	Višestruka regresijska analiza	Viša razina digitalne pismenosti povezana je s nižim povjerenjem u sigurnosne strategije digitalnih platformi.	Potvrđena
H2	Višestruka regresijska analiza	Percepcija manipulacije pokazala se statistički značajnim negativnim prediktorom povjerenja korisnika.	Potvrđena
H3	Hijerarhijska regresijska analiza i moderacijski model	Interakcijski učinak percepcije rizika i algoritamske svijesti pokazao se statistički značajnim, što potvrđuje moderirajuću ulogu percepcije rizika.	Potvrđena
H4	Analiza varijance (ANOVA)	Utvrđene su statistički značajne razlike u percepciji sigurnosnih strategija među korisnicima različitih razina digitalne pismenosti.	Potvrđena
H5	Analiza varijance (ANOVA)	Utvrđene su statistički značajne razlike prema spolu u percepciji sigurnosnih strategija digitalnih platformi.	Potvrđena

Kao što je prikazano u Tablici 7, svih pet hipoteza potvrđeno je na temelju provedenih analiza. Pritom su H1 i H2 potvrđene višestrukom regresijskom analizom, H3 hijerarhijskim i moderacijskim modelom, dok su H4 i H5 potvrđene analizom razlika među skupinama.

Dodatni rezultati analize varijance prikazani su u Tablici 8.

Tablica 8. Analiza varijance (ANOVA) razlika u percepciji sigurnosnih strategija prema spolu i razini digitalne pismenosti

Usporedba	F	df	p-vrijednost	Zaključak
Spol	33,64	(1, 521)	< .01	Statistički značajna razlika
Razina digitalne pismenosti	70,56	(2, 520)	< .001	Statistički značajna razlika

Kao što pokazuje Tablica 8, percepcija sigurnosnih strategija digitalnih platformi značajno se razlikuje prema spolu i razini digitalne pismenosti. Statistički značajna razlika utvrđena je prema spolu, $F(1, 521) = 33,64$, $p < .01$, što sugerira da procjene digitalne sigurnosti uključuju i rodno specifične obrasce osjetljivosti na rizik. Još izraženiji učinak utvrđen je za razinu digitalne pismenosti, $F(2, 520) = 70,56$, $p <$

.001, čime se dodatno potvrđuje da se povjerenje u digitalne platforme i percepcija njihovih sigurnosnih mehanizama oblikuju u skladu sa stupnjem korisničke informiranosti, iskustva i kritičke refleksije. U cjelini gledano, ovi nalazi podupiru tvrdnju da sigurnosne procjene u digitalnom okruženju nisu univerzalne, nego društveno i kognitivno strukturirane.

DISKUSIJA

Paradoks algoritamske svijesti i interpretacija nalaza

Rezultati višestruke i hijerarhijske regresijske analize, uz dodatnu provjeru odnosa među varijablama unutar predloženog modela, potvrđuju središnju tezu rada da se povjerenje korisnika u sigurnosne strategije digitalnih platformi ne oblikuje linearno, nego kroz međuigru digitalne pismenosti, percepcije manipulacije, percepcije rizika i algoritamske svijesti. Dobiveni nalazi pokazuju da viša razina digitalne pismenosti ne vodi nužno većem povjerenju, nego je povezana s izraženijom skepsom prema sigurnosnim mehanizmima platformi. Time se potvrđuje koncept paradoksa algoritamske svijesti: što korisnici bolje razumiju logiku algoritamskog upravljanja sadržajem i podacima, to su osjetljiviji na netransparentnost, manipulativne obrasce i ograničenja institucionalne zaštite.

Posebno je važan nalaz da se percepcija manipulacije pokazala najsnažnijim negativnim prediktorom povjerenja. Taj nalaz podudara se s prethodnim istraživanjima koja upozoravaju da korisničko nepovjerenje raste kada algoritamske odluke djeluju neobjašnjivo, nepravedno ili prikriveno usmjeravaju ponašanje korisnika (Bozdag, 2013; Binns i dr., 2018; Eslami i dr., 2017; Tufekci, 2014). U tom smislu, povjerenje u digitalne sustave ne ovisi samo o formalnom postojanju sigurnosnih protokola, nego o tome doživljavaju li ih korisnici kao legitimne, razumljive i usklađene s njihovim očekivanjima privatnosti i autonomije.

Nalazi o percepciji rizika dodatno produbljuju tu interpretaciju. Moderacijski učinak percepcije rizika pokazuje da algoritamska svijest sama po sebi ne povećava povjerenje; naprotiv, kada je praćena pojačanom sviješću o zloupotrebi podataka i sigurnosnim prijetnjama, povezana je s daljnjim smanjenjem povjerenja. Takav obrazac u skladu je s teorijom kontekstualnog integriteta, prema kojoj se procjene privatnosti i sigurnosti ne oblikuju apstraktno, nego u konkretnim društvenim i informacijskim kontekstima (Nissenbaum, 2023). Istodobno, nalazi se mogu povezati i s tzv. privatnosnim paradoksom, koji pokazuje da izražena zabrinutost za privatnost ne mora voditi povlačenju iz digitalnih sustava, nego koegzistira s njihovim intenzivnim korištenjem (Barth i de Jong, 2017).

Upravo se tu otvara šire sociološko značenje algoritamske svijesti. Ovaj rad pokazuje da digitalna pismenost nije samo funkcionalna kompetencija, nego oblik kulturnog i kognitivnog kapitala koji korisnicima omogućuje da prepoznaju skrivene obrasce moći u digitalnim okruženjima. Međutim, kako upozoravaju Gran, Booth i Bucher (2021), algoritamska svijest nije ravnomjerno raspodijeljena, nego može djelovati i kao nova os digitalne nejednakosti. U tom kontekstu, veća informiranost ne znači nužno veću sigurnost, nego često veću izloženost osjećaju epistemološke nesigurnosti, jer korisnik jasnije prepoznaje rizike, netransparentnost i mogućnosti manipulacije.

Dobiveni rezultati također potvrđuju da su spol i razina digitalne pismenosti važni za razumijevanje razlika u percepciji sigurnosnih strategija. Statistički značajne razlike prema spolu i razini digitalne pismenosti upućuju na to da sigurnosne procjene nisu univerzalne, nego društveno strukturirane. Nalaz o izraženijoj osjetljivosti sudionica prema sigurnosnim rizicima može se povezati s ranijim istraživanjima o rodnim razlikama u digitalnom povjerenju, privatnosti i procjeni rizika (Beldad i dr., 2010; Kamara i Kosta, 2016). Istodobno, rezultati koji pokazuju veći skepticizam digitalno pismenijih korisnika dodatno potvrđuju da se algoritamsko povjerenje ne može svesti na pitanje tehničke učinkovitosti, nego ga treba promatrati kao misaoni i društveni odnos prema sustavu.

Dodatna provjera odnosa među varijablama unutar predloženog modela ojačala je interpretativnu vrijednost nalaza te pokazala da se povjerenje oblikuje kroz povezane učinke digitalne pismenosti, percepcije rizika, percepcije manipulacije i njihova međudjelovanja. Time se potvrđuje da predloženi model ne funkcionira samo kao teorijska konstrukcija, nego i kao analitički održiv okvir za razumijevanje povjerenja u digitalnim interakcijama. U tom smislu, glavni doprinos rada nije samo u potvrdi pojedinih hipoteza, nego u tome što povjerenje redefinira kao rezultat interakcije znanja, osjetljivosti na manipulaciju i subjektivne procjene rizika, a ne kao automatsku posljedicu digitalne kompetencije.

Implikacije, izazovi i daljnja istraživanja

Dobiveni nalazi imaju teorijske, regulatorne i praktične implikacije. Teorijski, rezultati podupiru pomak od tehničkog prema komunikacijskom i sociološkom razumijevanju digitalne sigurnosti. Ako viša razina digitalne pismenosti povećava skepsu, tada povjerenje u digitalne platforme ne može biti objašnjeno samo prisutnošću sigurnosnih mjera, nego i načinom na koji korisnici interpretiraju njihovu svrhu, transparentnost i legitimnost. Time se potvrđuje važnost pristupa koji povezuju digitalnu sociologiju, etiku tehnologije i studije povjerenja (Floridi, 2023; Lyon, 2021; Masur, 2018).

Regulatorno gledano, rezultati upućuju na ograničenja modela zaštite privatnosti koji se oslanja isključivo na formalna pravila i informacijske obavijesti. Ako korisnici s višom razinom algoritamske svijesti i percepcije rizika pokazuju niže povjerenje, tada sama regulacija nije dovoljna ako ne proizvodi i doživljaj stvarne objašnjivosti, kontrole i odgovornosti. U tom smislu, ovi nalazi podupiru rasprave o potrebi za snažnijom algoritamskom transparentnošću, odgovornom primjenom umjetne inteligencije i regulatornim okvirima koji nadilaze formalno ispunjavanje obveza te uključuju jasnije standarde odgovornosti i upravljanja rizicima kroz cijeli životni ciklus sustava (Goodman i Flaxman, 2017; Koops, 2014; Leslie, 2020; OECD, 2023; National Institute of Standards and Technology, 2023; Taddeo i Floridi, 2018). Takav pristup pretpostavlja da povjerenje ne proizlazi samo iz formalne usklađenosti s pravilima, nego i iz sposobnosti institucija i platformi da rizike učine prepoznatljivima, upravljivima, i korisnicima barem djelomično objašnjivima. Posebno je važno upozorenje Wachtera i dr., (2017) da GDPR ne jamči funkcionalno pravo na objašnjenje, što dodatno pojačava jaz između regulatorne norme i korisničkog iskustva.

Praktične implikacije rada odnose se ponajprije na dizajn sigurnosnih strategija i edukacijskih intervencija. Rezultati sugeriraju da korisnike ne treba promatrati kao homogenu skupinu kojoj je dovoljno pružiti više informacija. Naprotiv, edukacija o digitalnoj sigurnosti mora biti diferencirana i usmjerena ne samo na jačanje kompetencija, nego i na razvoj interpretativne sposobnosti razumijevanja algoritamskih procesa, procjene rizika i prepoznavanja manipulativnih praksi (Diakopoulos, 2016; Elrayah i Jamil, 2023). U tom smislu, platforme i regulatori trebali bi razvijati pristupe koji istodobno povećavaju transparentnost, smanjuju informacijsku asimetriju i osnažuju korisnike za refleksivno digitalno odlučivanje.

Rezultati također otvaraju pitanje šire društvene cijene algoritamskog upravljanja. U uvjetima sve veće personalizacije, prediktivnog modeliranja i automatiziranog odlučivanja, povjerenje postaje povezano s osjećajem autonomije i mogućnošću kritičkog otpora (Sundar i Marathe, 2010). To znači da se digitalna sigurnost ne može više promatrati samo kao zaštita sustava, nego i kao zaštita korisničke sposobnosti da razumije, procijeni i ospori logiku sustava. U tom kontekstu, rezultati rada mogu se povezati s recentnim raspravama o informacijskim operacijama, hibridnim prijetnjama i političkoj ekonomiji digitalnih platformi, koje pokazuju da je povjerenje danas i sigurnosno i demokratsko pitanje (Rid, 2020; Zuboff, 2019).

Buduća istraživanja trebala bi se usmjeriti na nekoliko smjerova. Prvo, potrebno je provesti longitudinalna istraživanja kako bi se utvrdilo mijenja li se odnos između digitalne pismenosti, algoritamske svijesti i povjerenja pod utjecajem novih regulatornih mjera i promjena u platformskom okruženju. Drugo, korisno bi bilo provesti komparativna istraživanja među različitim platformama i tipovima digitalnih usluga,

jer je moguće da se obrasci povjerenja razlikuju između društvenih mreža, digitalnog bankarstva, e-trgovine i cloud servisa. Treće, važno je dodatno istražiti kako se algoritamska svijest razlikuje među društvenim skupinama, osobito u odnosu na obrazovanje, spol i različite oblike digitalnog kapitala. Konačno, bilo bi korisno razviti i testirati personalizirane edukacijske modele koji ne podižu samo razinu znanja, nego i sposobnost korisnika da kritički interpretiraju sigurnosne i etičke implikacije algoritamskog odlučivanja.

U cjelini gledano, diskusija potvrđuje da se paradoks algoritamske svijesti ne iscrpljuje u tvrdnji da "više znanja znači manje povjerenja", nego otkriva dublju napetost između informiranosti, autonomije i legitimnosti u digitalnom društvu. Upravo u tome leži širi doprinos rada: povjerenje u digitalne platforme pokazuje se kao društveno i komunikacijski posredovan odnos, oblikovan ne samo tehničkim rješenjima, nego i načinom na koji korisnici razumiju logiku digitalne moći.

ZAKLJUČAK

Ovo istraživanje potvrđuje da algoritamsko povjerenje nije neutralan ni tehnički uvjetovan odnos korisnika i digitalne infrastrukture, već kompleksan sociološki fenomen koji proizlazi iz distribucije znanja, moći i pristupa informacijama. Rezultati jasno pokazuju da viša razina digitalne pismenosti ne vodi automatiziranom povjerenju u sigurnosne strategije platformi, već je povezana s većom skepsom, kritičnijom procjenom rizika i izraženijim odmakom od nekritičkog prihvaćanja platformskih sigurnosnih mehanizama. S druge strane, korisnici s nižim razinama pismenosti iskazuju višu razinu povjerenja, što potvrđuje postojanje asimetrije u digitalnom iskustvu temeljene na kulturnom kapitalu. Povjerenje se u digitalnoj sferi pokazuje kao društveno strukturiran mehanizam, ukorijenjen u obrasce obrazovanja, pristupa znanju i interpretativne autonomije korisnika.

Korištenjem modela paradoksa algoritamske svijesti, istraživanje nudi teorijski doprinos razumijevanju dinamike povjerenja u kontekstu sveprisutne algoritamske obrade podataka. Povjerenje u digitalne sustave, kako se ovdje teorijski uokviruje, ne temelji se isključivo na funkcionalnim očekivanjima od tehnologije, nego i na normativnim poredcima koji određuju što se u digitalnom društvu smatra legitimnim znanjem, a što manipulacijom. Time se digitalna pismenost definira ne kao skup operativnih vještina, već kao kognitivni potencijal za kritičko razlučivanje rizika i autonomno donošenje odluka.

Nalazi dodatno potvrđuju rodnu dimenziju digitalnog povjerenja: žene pokazuju izraženiju osjetljivost prema sigurnosnim rizicima, što upućuje na potrebu za rodno osviještenim pristupom digitalnoj edukaciji i regulaciji. Ujedno se otvara pitanje epistemološke nejednakosti: viša razina znanja može povećati kritičnost i smanjiti

povjerenje, dok niža razina informiranosti može povećati izloženost manipulativnim praksama. Ovaj rad doprinosi digitalnoj sociologiji razradom misaonog modela povjerenja koji povezuje znanje, rizik i nejednakost u digitalnom prostoru. Povjerenje se tako prikazuje kao društveno oblikovana praksa otpora, a ne kao nekritičko prihvaćanje tehnoloških rješenja. Paradoks algoritamske svijesti razotkriva ključnu točku napetosti suvremenog digitalnog društva: povjerenje više nije tehničko pitanje, već misaoni čin unutar kulturno strukturiranog rizika. Upravo u tom misaonom obratu leži središnji doprinos ovog rada: digitalna sigurnost više nije pitanje protokola, već pitanje percepcije, a povjerenje u digitalne platforme ne počiva na onome što sustavi nude, već na onome što korisnici odluče vjerovati.

Paradoks algoritamske svijesti pokazuje da više znanja o digitalnim sustavima ne proizvodi nužno više povjerenja, nego može povećati osjetljivost na rizike, netransparentnost i manipulativne obrasce. U tom smislu, digitalna autonomija ne ovisi samo o mogućnosti korištenja tehnologije, nego i o sposobnosti kritičkog razumijevanja njezine logike i posljedica.

FINANCIRANJE

Ovaj rad nije financiran iz vanjskih izvora. Autorica je istraživanje provela samostalno, bez potpore znanstvenih projekata ili institucija.

SUKOB INTERESA

Autorica izjavljuje da ne postoji sukob interesa u vezi s ovim istraživanjem, njegovim autorstvom ili objavom.

ETIČKO ODOBRENJE

Istraživanje nije zahtijevalo formalno etičko odobrenje, budući da se temeljilo na anonimnom anketnom prikupljanju podataka bez osjetljivih osobnih informacija. Pri provedbi istraživanja poštovana su temeljna načela etike istraživanja, uključujući dobrovoljnost sudjelovanja, anonimnost i povjerljivost podataka.

PRISTUP PODACIMA I TRANSPARENTNOST

Podaci i dodatni materijali korišteni u ovom istraživanju dostupni su na zahtjev kod autorice.

LITERATURA

Acquisti A, Gritzalis S, Lambrinoudakis C i di Vimercati SDC (ur.). (2008). *Digital Privacy: Theory, Technologies, and Practices*. Boca Raton, FL: CRC Press.

Bakshy E, Messing S i Adamic LA (2015). Exposure to Ideologically Diverse News and Opinion on Facebook, *Science*, 348 (6239): 1130–1132. https://doi.org/10.1126/science.aaa1160

Barth S i de Jong MDT (2017). The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior - a Systematic Literature Review, *Telematics and Informatics*, 34 (7): 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bauer JM i Van Eeten MJG (2009). Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options, *Telecommunications Policy*, 33 (10–11): 706–719. https://doi.org/10.1016/j.telpol.2009.09.001

Beldad A, de Jong M i Steehouder M (2010). How Shall I Trust the Faceless and the Intangible? A Literature Review on the Antecedents of Online Trust, *Computers in Human Behavior*, 26 (5): 857–869. https://doi.org/10.1016/j.chb.2010.03.013

Bennett CJ i Raab C (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press.

Binns R, Veale M, Van Kleek M i Shadbolt N (2018). "It's Reducing a Human Being to a Percentage": Perceptions of Justice in Algorithmic Decisions, *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3173574.3173951

Boban M (2019). *Zaštita podataka i pravo na privatnost u informacijskom društvu*. Gospić: Veleučilište Nikola Tesla.

Borgesius FJZ, Trilling D, Möller J, Bodó B, de Vreese CH i Helberger N (2016). Should We Worry About Filter Bubbles?, *Internet Policy Review*, 5 (1). https://doi.org/10.14763/2016.1.401

Bozdag E (2013). Bias in Algorithmic Filtering and Personalization, *Ethics and Information Technology*, 15 (3): 209–227. https://doi.org/10.1007/s10676-013-9321-6

Bucher T (2018). *If... Then: Algorithmic Power and Politics*. Oxford: Oxford University Press.

Büchi M, Just N i Latzer M (2017). Caring Is Not Enough: The Importance of Internet Skills for Online Privacy Protection, *Information, Communication & Society*, 20 (8): 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Cath C (2018). Governing Artificial Intelligence: Ethical, Legal, and Technical Opportunities and Challenges, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376 (2133): 20180080. https://doi.org/10.1098/rsta.2018.0080

Diakopoulos N (2016). Accountability in Algorithmic Decision Making, *Communications of the ACM*, 59 (2): 56–62. https://doi.org/10.1145/2844110

Eslami M, Vaccaro K, Karahalios K i Hamilton K (2017). "Be Careful; Things Can Be Worse than They Appear": Understanding Biased Algorithms and Users' Behavior Around Them in Rating Platforms. *Proceedings of the International AAAI Conference on Web and Social Media*, 11 (1): 62–71. https://doi.org/10.1609/icwsm.v11i1.14898

Elrayah M i Jamil S (2023). Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness, *International Journal of Cyber Criminology*, 17 (2): 235–256. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/205 (25. svibnja 2024.)

European Union Agency for Cybersecurity (ENISA) (2024). *ENISA Threat Landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (7. svibnja 2024.)

Floridi L (2023). *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford: Oxford University Press.

Giannopoulos G, Smith H i Theocharidou M (2021). *The Landscape of Hybrid Threats. A Conceptual Model: public version*. Luxembourg: Publications Office of the European Union. https://doi.org/10.2760/44985

Goodman B i Flaxman S (2017). European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation", *AI Magazine*, 38 (3): 50–57. https://doi.org/10.1609/aimag.v38i3.2741

Gran A-B, Booth P i Bucher T (2021). To Be or Not to Be Algorithm Aware: A Question of a New Digital Divide?, *Information, Communication & Society*, 24 (12): 1779–1796. https://doi.org/10.1080/1369118X.2020.1736124

Jensen C, Potts C i Jensen C (2005). Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior, *International Journal of Human-Computer Studies*, 63 (1–2): 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Kamara I i Kosta E (2016). Do Not Track Initiatives: Regaining the Lost User Control, *International Data Privacy Law*, 6 (4): 276–290. https://doi.org/10.1093/idpl/ipw019

Koops B-J (2014). The Trouble with European Data Protection Law, *International Data Privacy Law*, 4 (4): 250–261. https://doi.org/10.1093/idpl/ipu023

Kumar N i Gupta R (2024). An Analysis of Consumers' Trusting Beliefs Towards the Use of E-Commerce Platforms: The Role of Security Measures, *Humanities and Social Sciences Communications*, 11: 95. https://doi.org/10.1057/s41599-024-03395-6

Leslie D (2020). *Understanding Artificial Intelligence Ethics and Safety: A Guide for the Responsible Design and Implementation of AI Systems*. The Alan Turing Institute. https://doi.org/10.5281/zenodo.3240529

Lyon D (2021). *Surveillance Society: Monitoring Everyday Life in the Digital Age*. Cambridge: Polity Press.

Masur PK (2018). *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments*. Cham: Springer. https://doi.org/10.1007/978-3-319-78884-5

National Institute of Standards and Technology (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg, MD: NIST. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf (5. svibnja 2024.)

Nissenbaum H (2019). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Nissenbaum H (2023). *Contextual Integrity: Revisiting Privacy in a Digital World*. Cambridge: Cambridge University Press.

OECD (2023). *Advancing Accountability in AI: Governing and Managing Risks Throughout the Lifecycle for Trustworthy AI*, *OECD Digital Economy Papers*, No. 349. Paris: OECD Publishing. https://doi.org/10.1787/2448f04b-en

Pariser E (2011). *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press.

Park YJ (2013). Digital Literacy and Privacy Behavior Online, *Communication Research*, 40 (2): 215–236. https://doi.org/10.1177/0093650211418338

Ribeiro MT, Singh S i Guestrin C (2016). Why Should I Trust You?: Explaining the Predictions of Any Classifier, *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1135–1144. https://doi.org/10.1145/2939672.2939778

Rid T (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.

Rubinstein IS (2011). Regulating Privacy by Design, *Berkeley Technology Law Journal*, 26 (3): 1409–1456. https://doi.org/10.15779/Z38368N

Schmitt MN (ur.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

Shaffer G (2021). Applying a Contextual Integrity Framework to Privacy Policies for Smart Technologies, *Journal of Information Policy*, 11: 222–265. https://doi.org/10.5325/jinfopoli.11.2021.0222

Smith HJ, Milberg SJ i Burke SJ (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices, *MIS Quarterly*, 20 (2): 167–196. https://doi.org/10.2307/249477

Sundar SS i Marathe SS (2010). Personalization Versus Customization: The Importance of Agency, Privacy, and Power Usage, *Human Communication Research*, 36 (3): 298–322. https://doi.org/10.1111/j.1468-2958.2010.01377.x

Taddeo M i Floridi L (2018). How AI Can Be a Force for Good, *Science*, 361 (6404): 751–752. https://doi.org/10.1126/science.aat5991

Tufekci Z (2014). Engineering the Public: Big Data, Surveillance and Computational Politics, *First Monday*, 19 (7). https://doi.org/10.5210/fm.v19i7.4901

U.S. Department of Defense (2023). 2023 DoD Cyber Strategy Summary. Washington, DC: U.S. Department of Defense. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf (12. lipnja 2024.)

Vosoughi S, Roy D i Aral S (2018). The Spread of True and False News Online, *Science*, 359 (6380): 1146–1151. https://doi.org/10.1126/science.aap9559

Wachter S, Mittelstadt B i Floridi L (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 7 (2): 76–99. https://doi.org/10.1093/idpl/ipx005

Zuboff S (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Revija za sociologiju | Croatian Sociological Review 55 (2025), 2: 121–144

The Paradox of Trust in Digital Platforms: Algorithmic Awareness in Digital Interactions

Marija GOMBAR https://orcid.org/0009-0000-8621-4007
General Staff of the Armed Forces of the Republic of Croatia
gombar.ma@gmail.com

ABSTRACT

This paper examines the relationship between digital literacy, perceived manipulation, risk perception, and algorithmic awareness in shaping users' trust in the security strategies of digital platforms. The theoretical framework is grounded in the concept of the paradox of algorithmic awareness, according to which greater knowledge of digital systems does not necessarily lead to higher trust, but may instead intensify scepticism and sensitivity to risk. The study was conducted on a sample of 523 participants aged 18 to 35, and the data were analysed using factor analysis, multiple and hierarchical regression analysis, analysis of variance, and structural equation modelling. The findings show that digital literacy, perceived manipulation, and risk perception are statistically significant negative predictors of trust in platform security strategies, with perceived manipulation emerging as the strongest negative predictor. A statistically significant moderating effect of risk perception on the relationship between algorithmic awareness and trust was also confirmed. In addition, significant differences were found by gender and level of digital literacy, with more digitally literate users expressing greater scepticism and female participants showing greater sensitivity to security risks. The main contribution of the paper lies in a model that explains trust in digital platforms as the outcome of the interplay between knowledge, perceived manipulation, and risk assessment, rather than as an automatic consequence of digital competence. The findings point to the need for approaches to digital security that simultaneously strengthen transparency, user autonomy, and critical understanding of algorithmic processes.

Key words: algorithmic awareness, digital literacy, digital security, trust in digital platforms, risk perception